동역학계를 이용한 난수열 발생 시스템

김재겸[†] · 조성진[††] · 김한두[†††] · 이경현[††††] · 손호준[†††††]

요 약

본 논문에서는 동역학계를 해석하는 방법들 중의 한가지인 다차원 셀룰라 오토마타에 기초한 난수열 발생 시스템을 제안하였다. 제안된 난수열 발생 시스템은 키의 사용이 요구되는 경우와 요구되지 않는 경우에 모두 적용이 가능하도록 구성되었으며, 키를 사용하는 경우 키의 크기는 128bits에서 256bits까지 가변적으로 사용할 수 있게 구성되었다. 제안된 난수열 발생 시스템의 수행속도는 Pentium MMX 200MHz (64M RAM, Windows 98) 환경에서 약 380Mbits/sec로 측정되었다.

Pseudo-random bit sequence generator based on dynamical systems

Jae Gyeom Kim[†], Sung Jin Cho[††], Han Doo Kim[†††], Kyung Hyune Rhee[††††] and Ho Jun Son[†††††]

ABSTRACT

In this paper, We proposed a pseudo-random bit sequence generator based on the concept of n-dimensional cellular automata which is a method of analyzing dynamical systems. The proposed generator is designed for using and disusing key. And the key size is variable from 128 bits to 256 bits. The generator was estimated to generate 380Mbits/sec under Pentium MMX 200MHz (64M RAM, Windows 98).

1. 서 론

현대 암호학의 많은 응용 분야들에서 통계적 성질들이 우수한 난수열의 생성은 중요한 부분을 차지하고 있다. 예를 들어 공개키 암호 시스템에서 사용자들의 키는 반드시 난수적 특성을 만족하여야 하며, 대칭키 암호 시스템의 일종인 스트림 암호 시스템에서는 비교적 짧은 길이의 사용자 키로부터 예측불가능하며, 긴 주기를 가지는 키 스트림의 생성은 필수 항목이다. 뿐만 아니라 스트림 암호 시스템에서 사용되는 난수 생성기는 그 응용분야의 특성상 빠른 생성 속도를 요구하고 있다. 또한 최근에는 대칭키 암호 시스템의 키 스케줄러의 약점을 이용한 공격법들이 소개되면서, 난수적 특성이 강하면서도 빠른 시간 안에 라운드 키를 생성해 낼 수 있는 난수 생성기의 필요성이 더욱 증대되고 있다.

셀룰라 오토마타(CA, Cellular Automata)란 동역학계를 해석하는 한 방법으로 공간과 시간을 이산적으로 다루고, 이산적 공간인 셀룰라 공간(Cellular Space)의 기본 단위인 각 셀(Cell)이 취할 수 있는 상태를 유한하게 처리하며, 각 셀의 상태가 국소적인 상호 작용에 의해서 동시에 갱신되는 시스템이다. CA는 셀들의 배열 방식에 따라 모든 셀들이 선형으로 배열되어 있는 1차원 CA와 셀들이 평면으로 구성되어 있는 2차원 CA, 그리고 셀들의 배열이 공간적으로 구성되어 있는 다차원 CA로 나눌 수 있다.

1차원 CA를 이용한 스트림 암호 알고리즘이 1985년 Wolfram에 의해서 최초로 제안된 후[1,2], 1994년

이 논문은 1998학년도 경성대학교 학술지원 연구비에 의하여 연구되었음.

† 정회원, 경성대학교 수리과학부
†† 정회원, 부경대학교 수리과학부
††† 정회원, 인제대학교 컴퓨터응용과학부
†††† 종신회원, 부경대학교 전자컴퓨터통신공학부
††††† 경성대학교 수리과학부

Nandi 등에 의해서 PCA(Programmable Cellular Automata)를 이용한 스트림 암호 알고리즘이 제안된 바 있고[3], 1997년 Mihaljević에 의해서 Nandi 등의 알고리즘을 개선한 스트림 암호 알고리즘이 제안된 바 있으며[4], 이에 관련된 연구들이 이루어져 왔다[5-7]. CA는 그 본질적인 특성이 확산과 국소적인 상호 작용이므로 암호 시스템과 VLSI(Very Large Scale Integrated circuit) 환경에 적합한 것으로 알려져 있으며[8], 다차원 CA는 그 구조의 복잡성으로 인해 분석이 어렵고, 각 셀의 상태가 다른 셀 들의 상태에 영향을 주는 속도가 1차원 CA에 비하여 훨씬 더 빠르므로 1차원 CA보다 암호 시스템에 적합하다. 그러나 현재까지의 CA의 암호 시스템에의 응용에 관한 연구는 주로 1차원 CA에 머물러 왔는데, 이는 1차원 CA의 이론적인 연구의 용이성 때문이다.

본 논문에서는 새로운 구조의 다차원 CA를 제안하고 이를 이용한 난수열 발생 알고리즘을 제안하고, 제안된 알고리즘으로부터 출력 난수열들에 대한 통계적 검증을 실시하였다.

본 논문의 구성은 다음과 같다. 2장에서는 새로운 구조의 다차원 CA를 제안하고, 3장에서는 이 구조를 이용한 난수열 발생 시스템을 제안하고, 4장에서는 제안된 시스템의 통계적 검증 결과를 밝히며, 5장은 결론이다.

2. 제안된 다차원 셀룰라 오토마타의 구조

본 연구에서 사용하고자 하는 CA의 셀룰라 공간은 그림 1에서와 같은 형태의 배열을 기초로 하며, 이때 점선으로 표시된 각각의 삼각형 Ci (i=0,…,9)들을 셀이라 한다.

Nest란 이웃하는 3개의 셀 들의 집합으로 그림 1
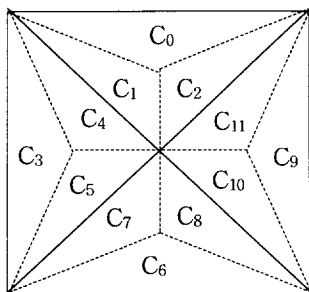
그림 1. Nest

의 실선으로 표시된 최소단위의 삼각형이다.

예를 들어 3개의 셀들이 집합 $\{C_0, C_1, C_2\}$가 하나의 Nest가 된다. 셀 C_i와 한 변을 공유하고 있는 3개의 셀 들을 셀 C_i의 이웃이라 하며, 셀 C_i의 이웃들은 셀 C_i의 다음 상태를 결정짓는 상태 전이 함수의 입력이 된다. 예를 들어 그림 1의 셀 C_7의 이웃이 되는 셀 들은 C_5, C_6, C_8이며 이들 중 C_6과 C_8은 같은 셀 C_7과 같은 Nest에 속해있다. 그림 1에서 C_0, C_3, C_6, C_9는 2개의 이웃을 가지며 이들을 제외한 나머지 셀들은 3개의 이웃을 가지게 되는데, 그림 1에서와 같이 전체 CA 공간의 경계부분이 되는 사각형의 각 변에 있는 셀들, 즉 C_0, C_3, C_6, C_9의 세 번째의 이웃을 결정해 주는 것을 CA의 경계조건이라 한다. 본 연구에서는 제일 위쪽 변과 제일 아래 쪽 변을 서로 이어 붙이고, 제일 왼쪽 변과 제일 오른쪽 변을 서로 붙이는 것으로 한다. 즉, C_0와 C_6이 서로의 세 번째 이웃이 되며, C_3와 C_9이 서로의 이웃이 되도록 구성한다. 이렇게 구성된 셀룰라 공간은 Torus의 표면에 각 셀의 이웃이 3개씩 되도록 삼각형의 셀 들이 빈틈없이 배열되어 있는 형태이다. 이러한 형태의 셀룰라 공간을 Torus에 기반한 셀룰라 공간이라 부르기로 한다.

Torus에 기반한 셀룰라 공간에서 정의된 CA의 특징은 각 셀의 이웃의 개수를 최소로 하면서도, 확산의 속도(즉, 각 셀의 상태가 다른 셀 들의 상태에 영향을 주는 단계)가 매우 빠르다는 데 있다.

Torus에 기반한 셀룰라 공간에서 지정된 셀들을 셀룰라 공간에서 삭제하는 것을 Cut이라하고, 2개의 셀을 Cut한 다음 Cut이 이루어진 서로 다른 셀에 속한 두 변들을 짝지어 붙이는 것을 Glue라 정의한다.

이렇게 2개의 셀을 Cut한 다음 절단 변들을 서로 짝지어 Glue하는 방법의 경우의 수는 6가지이다. Cut And Glue 기법을 적용한다는 것은 이와 같은 방법으로 짝수개의 셀을 Cut한 다음, 삭제된 셀을 2개씩 서로 대응시키고, 대응되는 셀의 절단 변끼리 서로 Glue한다는 것이다.

Torus 기반의 셀룰라 공간에 Cut And Glue 기법을 적용할 경우 확산 현상의 불규칙성과 확산시의 간섭 효과의 불규칙성을 극대화할 수 있다.

3. 제안된 난수열 발생 시스템

3.1. 셀룰라 공간

그림 2와 같이 삼각형들로 분할되어 있는 평면도
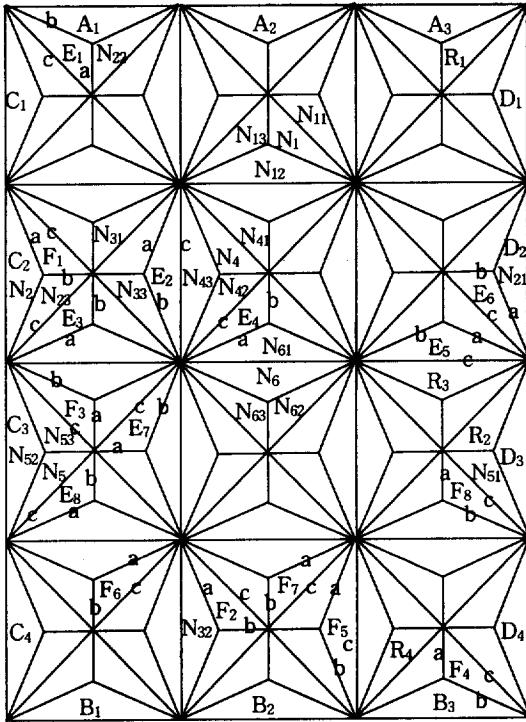
그림 2. 셀룰라 공간 SPRA

형을 Cut and Glue 기법을 이용하여 아래의 단계 1과 같이 조작 변형한 다음 단계 2와 같은 방법으로 추가로 조작 변형한 공간을 셀룰라 공간 SPRA라 한다.

단계 1(경계 조건) : A_1, A_2, A_3 삼각형의 위쪽 변을 각각 B_1, B_2, B_3 삼각형의 아래쪽 변에 이어 붙이고, 그림 2의 C_1, C_2, C_3, C_4 삼각형의 왼쪽 변을 각각 그림 2의 D_1, D_2, D_3, D_4 삼각형의 오른쪽 변에 이어 붙여서 Torus에 기반한 셀룰라 공간을 만든다.

단계 2(Cut and Glue) : 그림 2의 E_1, E_2, E_3, E_4, E_5, E_6, E_7, E_8, F_1, F_2, F_3, F_4, F_5, F_6, F_7, F_8 삼각형의 내부를 각각 삭제한 다음, 그림 1의 E_1, E_2, E_3, E_4, E_5, E_6, E_7, E_8 삼각형의 변 a, b, c를 각각 그림 2의 F_1, F_2, F_3, F_4, F_5, F_6, F_7, F_8 삼각형의 변 a, b, c에 각각 이어 붙인다.

이렇게 하여 만든 도형이 난수 발생 시스템에서사용하는 셀룰라 공간 SPRA이다. 이 셀룰라 공간 SPRA는 최소 단위의 삼각형을 128개 가지며, 이 최소 단위의 삼각형 각각이 셀룰라 공간 SPRA의 셀이 되며, 128개의 셀들에 대한 번호는 0에서 127까지 사전에 부여한다.

3.2. 동시변환 규칙

앞에서 정의된 셀룰라 공간 SPRA의 각 셀의 값들을 시각의 변화에 따라 동시에 갱신하는 규칙들을 동시 변환 규칙이라고 하며, 본 논문에서 사용하는 동시 변환 규칙은 동시 변환 규칙 RAL과 동시 변환 규칙 RANL 그리고 동시 변환 규칙 RAR이다.

3.2.1. 선형 동시변환 규칙

동시변환 규칙 RAL은 셀룰라 공간 SPRA의 셀들의 값들을 시각의 변화에 따라 동시에 갱신하는 규칙들 중의 하나로, 시각 t에서 모든 셀 들의 값들이 주어져 있을 때, 시각 t+1에서의 각 셀의 값으로 그 셀과 인접하는 3개의 셀들의 시각 t에서의 값들을 bitwise하게 XOR(배타적논리합)한 값을 부여하는 것으로 선형 규칙이다.

3.2.2. 비선형 동시변환 규칙

동시변환 규칙 RNL은 셀룰라 공간 SPRA의 셀들의 값들을 시각의 변화에 따라 동시에 갱신하는 규칙들 중의 하나로, 시각 t에서 모든 셀들의 값들이 주어져 있을 때, 그림 1의 N_i(i=1, 2, 3, 4, 5, 6) 의 6개의 셀들의 경우는 시각 t+1에서의 셀 N_i의 값으로 시각 t에서의 셀 N_{i1}의 값과 셀 N_{i2}의 값을 bitwise하게 XOR(논리합)한 후 이 논리합을 시각 t에서의 셀 N_{i3}의 값과 bitwise하게 XOR한 값을 부여하고, 이 6개의 셀들을 제외한 나머지 셀들의 시각 t+1에서의 값들은 위의 동시변환 규칙 RAL의 방법으로 부여하는 규칙으로 비선형 규칙이다.

3.2.3. Rotation에 의한 동시변환 규칙

동시변환 규칙 R은 셀룰라 공간의 셀들의 값들을 시각의 변화에 따라 동시에 갱신하는 규칙들 중의 하나로, 시각 t에서 모든 셀들의 값들이 주어져 있을 때, 그림 1의 R_1, R_2, R_3, R_4 셀의 시각 t+1에서의 값으로 각각 R_1, R_2, R_3, R_4 셀의 시각 t에서의 값을 각각 3bit, 5bit, 7bit, 13bit 씩 상위 bit 방향으로 bitwise rotation한 값을 부여하고, 이 4개의 셀들을 제외한 나머지 셀들의 값들은 변화시키지 않는 규칙으로 선형 규칙이다.

3.3. 셀들의 초기 값 부여

셀룰라 공간 SPRA의 셀 들의 초기 값의 부여는 각 셀에 32bits의 값을 부여하는 것으로 한다. 셀룰라 공간 SPRA는 128개의 셀 들로 구성되어 있으므로 셀들의 초기 값으로 부여할 수 있는 총 bit 수는 4096 (=128×32)이다. 이 초기 값의 부여는 현재 시각 등 여러 가지 요소들을 이용하여 부여할 수 있다.

3.4. 키 값의 반영 방법

3.4.1. 키 값의 반영 방법 1

초기 값이 부여되어 있는 셀룰라 공간 SPRA의 셀들에 키 값을 반영시키는 방법들 중의 하나로, 키 값을 이진 bit의 열로 표현했을 때, 최하위 bit를 기준으로 i번째 bit의 값이 1이면 i_1번 셀의 값의 최상위 bit를 기준으로 i_2번째 bit의 값을 1로 부여하고 i_1번 셀의 값의 최상위 bit를 기준으로 i_3번째 bit의 값을 0으로 부여하며, i번째 bit의 값이 0이면 i_1번 셀의 값의 최상위 bit를 기준으로 i_2번째 bit의 값을 0으로 부여하고 i_1번 셀의 값의 최상위 bit를 기준으로 i_3번째 bit의 값을 1로 부여한다. 단,

$$i = 128 \times q_1 + i_1 \quad (0 \le i_1 < 128),$$
$$i+q_1 = 32 \times q_2 + i_2 \quad (0 \le i_2 < 32),$$
$$i_2+16 = 32 \times q_3 + i_3 \quad (0 \le i_3 < 32)$$

이고, i, i_1, i_2, i_3 등의 counting은 0부터 시작한다. 여기서 유효한 키 값의 최대 길이는 2048(=128×16) bits이다.

3.4.2. 키 값의 반영 방법 2

초기 값이 부여되어 있는 셀룰라 공간 SPRA의 셀들에 키 값을 반영시키는 방법들 중의 하나로, 키 값을 이진 bit의 열로 표현했을 때, 최하위 bit 를 기준으로 i번째 bit의 값이 1이면 i_1번 셀의 값의 최상위 bit를 기준으로 i_2번째 bit의 값에 1을 XOR하고, i번째 bit의 값이 0이면 i_1번 셀의 값의 최상위 bit를 기준으로 i_3번째 bit의 값에 1을 XOR한다. 단, i_1, i_2, i_3은 키 값의 반영 방법 RAK1에서의 i_1, i_2, i_3와 동일하며, i, i_1, i_2, i_3 등의 counting은 0부터 시작한다. 여기서 유효한 키 값의 최대 길이는 2048(=128×16)bits이다.

3.5. 난수 열의 값의 추출 방법

셀룰라 공간 SPRA의 셀들의 값들로부터 난수 열을 구성하는 값들을 추출하는 방법 RAE는 셀룰라 공간 SPRA의 전체 셀들 중 사전에 지정된 일부의 셀들의 값들을 추출하는 방법이며, 이렇게 출력된 32비트의 값들이 난수열 발생 시스템의 최종 출력이 된다. 여기서는 전체 128개의 셀들 중 3/4인 96개의 셀들을 사전에 지정한다. 따라서 값들을 추출하는 방법 RAE의 1회의 실행에 의하여 추출되는 양은 3072(=96×32)bits이다.

3.6. 제안된 난수열 발생 시스템

제안된 난수열 발생 시스템의 난수열 발생 알고리즘을 단계별로 정리하면 아래와 같다.

단계 1 : 셀룰라 공간 SPRA의 셀들의 초기 값 부여

단계 2 : 키를 RAK1의 방법(또는 RAK2의 방법)에 의하여 셀룰라 공간 SPRA의 셀 들의 값들에 반영

단계 3 : 셀룰라 공간 SPRA의 셀 들의 값들을 규칙 RAL에 의하여 1회 갱신한 뒤 규칙 RAR에 의하여 1회 갱신하는 것을 10회 반복

단계 4 : 셀룰라 공간 SPRA의 셀 들의 값들을 규칙 RNL에 의하여 1회 갱신한 뒤 규칙 RAR에 의하여 1회 갱신

단계 5 : 셀룰라 공간 SPRA의 셀들의 값들로부터 RAE의 방법에 의해서 3072 bits의 값을 추출

단계 6 : 추출이 더 필요하면 단계 4로

단계 7 : Stop

4. 제안된 난수열 발생 시스템의 분석 및 검정

4.1. 제안된 시스템 분석

셀룰라 공간 SPRA의 기하적 구조는 가능한 다양한 구조들 중 여러 가지 이론적 · 실험적인 연구와 분석에 의해서 효율적인 것으로 선택된 구조이다.

동시변환 규칙 RAL은 셀들의 값들을 확산시키는 속도가 매우 빠른 것으로 분석되었으며, 이에 따라 셀룰라 공간 SPRA의 셀들의 값들을 초기 혼합하는 과정인 알고리즘의 단계 3에 규칙 RAL을 적용하였다. 알고리즘의 단계 3과 단계 4에서 적용되는 동시변환 규칙 RAR은 셀들의 값들의 각 bit의 값이 모든

셀들의 모든 위치의 bit들에 효율적으로 영향을 미치도록 구성되었으며, 규칙 RAR에서의 rotation의 개수, 위치, bit size 등은 실험적인 분석에 의하여 최적화된 것이다. 동시변환 규칙 RANL은 비선형적인 규칙으로 규칙 RAL과 RAR이 모두 선형적이라는 약점을 보완하기 위하여 구성된 것으로, 비선형적인 요소들을 적절히 가미하면서도 규칙 RAL의 장점을 최대한 살릴 수 있도록 구성되었으며, 비선형적인 요소들을 적절히 가미하는 구체적인 방법은 실험적인 분석에 의하여 최적화된 것이다.

키 값의 반영 방법 RAK1과 RAK2는 알고리즘에 의해서 생성되는 난수들이 키 값을 효율적으로 반영할 수 있도록 구성되었으며, 각각 장단점이 있다. 이러한 RAK1과 RAK2의 두 가지의 방법 모두에서 키의 size는 0bit에서 2048bits까지 가변적으로 사용될 수 있다. 여기서 키의 size가 0bit인 경우는 키를 사용하지 않는 경우이다. 그리고 알고리즘의 구현 시에 두 가지 방법들 중 한 가지 방법을 선택하도록 하였다.

난수 열의 값의 추출하는 방법 RAE에서는 셀룰라 공간 SPRA의 전체 셀들 중 3/4을 이용하는데, 이는 추출한 난수들의 상호 종속성을 단절시키면서도 알고리즘의 수행 속도를 높이기 위한 것이다.

이러한 제안된 난수열 발생 시스템은 기존의 난수열 발생 시스템들에서는 찾아볼 수 없는 새로운 형태의 독창적인 시스템이며, 불규칙성의 생성, 불규칙성의 효과적인 확산, 확산의 상호 간섭효과 등을 극대화하여 임의성이 우수한 난수열을 효과적으로 생성할 수 있는 시스템인 것으로 분석된다.

4.2 제안된 시스템의 통계적 검정

4.2.1. 실험 방법

제안된 난수열 발생 시스템의 통계적 검정을 위하여, 시스템의 출력 난수열들에 대한 빈도 검정(Frequency Test), 포커 검정(Poker Test), 런 검정(Run Test), 롱런 검정(Long Run Test), 계열 검정(Serial Test), 자기상관 검정(Autocorrelation Test) 등의 통계적 검정들을 시행하였으며, 제안된 시스템의 수행 속도를 측정하였다.

사용된 알고리즘의 단계 1에서의 셀룰라 공간 SPRA의 셀들의 초기 값들은 모든 셀들의 최하위 비트와 최상위 비트에는 1의 값을 주고 나머지 비트들에는 0의 값을 방법으로 부여하였으며, 알고리즘의 단계 2에서의 키를 셀룰라 공간 SPRA 의 셀들의 값들에 반영하는 방법은 RAK1의 방법을 적용하였으며, 사용된 키들의 size는 128bits이며, 사용된 키들은 C++에서 제공하는 rand()함수를 이용하여 구한 난수들을 이용하여 생성하였다.

그리고 통계적 검정들에서 사용된 표본 1은 개발된 알고리즘에 키를 10000개 사용하여 출력되는 각 수열에서 하나씩의 표본을 추출한 10000개의 표본들로 구성하였으며, 각 수열에서 하나의 표본을 추출하는 방법은 각 수열의 최초의 20000bits를 추출하는 방법을 사용하였다. 통계적 검정들에서 사용된 표본 2는 개발된 알고리즘에 키를 사용하지 않고 출력되는 수열을 처음부터 순서대로 20000bits씩 나눈 10000개의 표본들로 구성하였다.

이와 같은 실험에서는 Visual C++ 6.0으로 구현된 알고리즘이 사용되었으며, Pentium MMX 200MHz 환경에서 실험되었다.

4.2.2. 통계적 검정 결과

표 1은 제안된 난수열 발생 시스템의 출력 난수열들에 대한 빈도 검정, 포커 검정, 런 검정, 롱런 검정, 계열 검정, 자기상관 검정 등의 검정들을 시행한 결과를 나타낸 것인데, 모든 경우에서 통과함을 알 수 있다. 이와 같은 검정 결과들로부터, 제안된 난수열 발생 시스템의 출력 난수열들의 임의성이 우수함을 알 수 있다. 표 1에서의 측정치 1과 측정치 2는 각각 위의 표본 1과 표본 2에서의 측정치이다.

표 1. 통계적 검정 결과

검정 방법	기준치 (유의수준 5%)	측정치 1 (keyed)	측정치 2 (non-keyed)
빈도 검정	$\chi^2<3.8415$	$\chi^2= 1.0983$	$\chi^2= 1.0801$
포커 검정 (m=4)	$\chi^2<24.9958$	$\chi^2=16.1594$	$\chi^2=16.1741$
런 검정	$\chi^2<41.3371$	$\chi^2=19.3156$	$\chi^2=19.4854$
롱런 검정	i<34 (i:최대런의길이)	i=14.6182	i=14.5912
계열 검정	$\chi^2<5.9915$	$\chi^2= 2.1363$	$\chi^2= 2.1542$
자기상관 검정	$\chi^2<5.9915$	$\chi^2= 3.2256$	$\chi^2= 3.0627$

4.2.3. 수행속도

제안된 난수열 발생 시스템의 수행속도는 Pentium MMX 200MHz(64M RAM, Windows 98) 환경에서 약 380Mbits/sec로 측정되었다. 이러한 속도는 알고리즘의 최적화가 이루어지지 않은 상태에서 측정된 것인데, 알고리즘의 최적화가 이루어지면 더욱 향상될 것으로 예상된다.

5. 결 론

본 논문에서는 새로운 구조의 다차원 셀룰라 오토마타를 제안하고, 제안된 다차원 셀룰라 오토마타를 이용한 난수열 발생 시스템을 제안하였다. 제안된 난수열 발생 시스템의 수행속도는 기존의 난수열 발생 시스템들과 비교하여 비교적 빠른 편이다. 셀룰라 오토마타의 특성상 하드웨어로 구현할 경우 더욱 빠른 수행속도를 기대할 수 있다. 또한 제안된 난수열 발생 시스템으로부터 생성된 난수열들의 난수적 특성을 조사하기 위하여 몇 가지 통계 테스트들을 수행하였다. 이러한 테스트의 결과 제안된 난수열 발생 알고리즘으로부터 생성된 난수들은 좋은 난수적 특성들을 가지고 있다는 것을 알 수 있었다.

참 고 문 헌

[1] S. Wolfram, "Cryptography with cellular automata", *Advances in Cryptology : Proc. of CRYPTO '85, Lecture Notes in Computer Science,* Vol. 218, pp.429-432, 1986.

[2] S. Wolfram, "Random sequence generation by cellular automata", *Advances in Applied Math,* Vol. 7, pp.123-169, 1986.

[3] S. Nandi, B.K. Kar and P.P. Chaudhuri, "Theory and application of cellular automata in cryptography," *IEEE Trans. Computers,* Vol. 43, pp.1346-1357, 1994.

[4] M.J. Mihaljević, "An imporved key stream generator based on the programmable cellular automata", *Information and Communication security-ICICS'97, Lecture Notes in Computer Science.* Vol. 1255, pp. 250-26, 1997.

[5] W. Meier and O. Staffelbach, "Analysis of pseudo random sequences generated by cellular automata", *Advances in Cryptology: Proc. of EUROCRYPTO '91, Lecture Notes in Computer Science,* Vol. 547, pp.186-199, 1992.

[6] M. Serra, T. Slater, J.C. Muzio and D.M. Miller, "The analysis of one-dimansional linear cellular automata and their aliasing properties", *IEEE Trans. Compter-Aided Design,* Vol. 9, pp.767-778, 1990.

[7] S. Nandi and P.P. Chaudhuri, "Analysis of periodic and intermediate boundary 90/150 celullar automata", *IEEE Trans. Computers,* Vol. 45, pp.1-12, 1996.

[8] P.D. Hortensius, R.D. McLeod and H.C. Card, "Parallel random number generation for VLSI systems using cellular automata", *IEEE Trans. Computers,* Vol. 38, pp.1466-1472, 1989.